Notas de la versión de Sentinel 7.3

Febrero de 2015



Sentinel 7.3 incluye nuevas funciones, aumenta la facilidad de uso y soluciona varios problemas anteriores.

Muchas de estas mejoras se realizaron en respuesta directa a las sugerencias de nuestros clientes. A todos les agradecemos su tiempo y su valiosa aportación. Esperamos que sigan ayudándonos a garantizar que nuestros productos satisfagan todas sus necesidades. Puede publicar comentarios en el foro de Sentinel en Comunidades de NetIQ, nuestra comunidad en línea que también incluye información sobre productos, blogs y enlaces a recursos útiles.

La documentación de este producto está disponible en el sitio Web de NetIQ en formato HTML y PDF, en una página que no requiere entrar a una sesión. Si tiene sugerencias de mejora para la documentación, haga clic en el botón para **comentar un tema** situado al final de cualquier página de la versión HTML de la documentación publicada en la página de de documentación de Sentinel NetIQ. Para descargar este producto, consulte el sitio Web de actualizaciones del producto Sentinel.

1 Novedades

En las secciones siguientes se describen las principales mejoras y funciones, además de los problemas que soluciona esta nueva versión:

1.1 Una sola plataforma unificada para Sentinel y Sentinel Log Manager

Ahora NetIQ proporciona Sentinel como una sola plataforma para las soluciones Sentinel y Sentinel Log Manager.

La plataforma Sentinel consta de dos soluciones principales:

- **Sentinel Enterprise:** completa solución que permite realizar análisis de seguridad en tiempo real y muchas otras funciones. Sentinel Enterprise se centra en los casos de uso de SIEM, como la detección de amenazas en tiempo real, las alertas y la corrección.
- **Sentinel for Log Management:** solución para casos de uso de gestión de registros, como las capacidades de recopilación, almacenamiento, búsqueda y notificación de datos.

NetIQ proporciona licencias independientes para cada una de estas soluciones. En el caso de instalaciones nuevas, la plataforma Sentinel habilita la funcionalidad según se introduzca una clave de licencia de Sentinel Enterprise o de Sentinel for Log Management. Este cambio no tiene ninguna repercusión en los servidores o actualizaciones existentes de Sentinel.

Para obtener más información sobre las funciones habilitadas en cada solución, consulte la sección “Understanding License Information ” (Información de licencia) de la *NetIQ Installation and Configuration Guide (Guía de instalación y configuración de NetIQ).*

1.2 Notificaciones de alerta y clasificación

Ahora es posible configurar reglas de correlación para recibir notificaciones de alerta instantáneas sobre amenazas potenciales. Las alertas le informan de los aspectos más importantes que debe atender. Pueden estar relacionadas con amenazas a recursos de TI o umbrales de rendimiento, como una memoria del sistema llena o recursos de TI que no responden. Sentinel asocia los eventos e identidades relevantes con la alerta automáticamente para ayudarle a determinar la causa raíz de la amenaza potencial.

Para obtener más información, consulte la sección “Configuring Alert Notifications” (Configuración de las notificaciones de alerta) de la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

Sentinel proporciona vistas de alertas en tiempo real en formato gráfico y tabular. Puede realizar operaciones de clasificación de alertas, cambiar el estado de una alerta, asignar alertas a usuarios o funciones, añadir información a la base de conocimientos, etc. Puede ver una vista más detallada de cada alerta que incluya, por ejemplo, los eventos activadores, las identidades de usuario implicadas y el historial de alertas. Para obtener más información acerca de la vista de alertas, consulte la sección “Viewing and Triaging Alerts in Alert Views” (Visualización y clasificación de alertas en la vista de alertas) en la “*NetIQ Sentinel User Guide (Guía del usuario de NetIQ Sentinel).*”

1.3 Consolas de alertas

Las consolas de alertas le permiten explorar y analizar a fondo las alertas. La consola de alertas constituye una interfaz personalizable y fácil de configurar donde puede ver e investigar las alertas en detalle. Por ejemplo, puede averiguar el tiempo medio que tardan los propietarios en cerrar las alertas, la regla de correlación que genera más alertas, el número medio de alertas consolidadas, las ubicaciones geográficas de las alertas de gravedad severa, y mucho más. Para obtener más información acerca de las consolas de alertas, consulte la sección "Analyzing Alert Dashboards" (Análisis de las consolas de alertas) en la "*NetIQ Sentinel User Guide (Guía del usuario de NetIQ Sentinel).*"

1.4 Vistas de eventos en tiempo real en la interfaz Web

Ahora puede ver eventos en tiempo real en la interfaz Web de Sentinel sin necesidad de entrar al Centro de control de Sentinel. Las vistas de eventos en tiempo real muestran un resumen de los datos de eventos. Para ver los detalles de un evento o realizar alguna operación de evento, puede utilizar la interfaz de búsqueda. Para obtener más información acerca de las vistas de eventos en tiempo real en la interfaz Web, consulte la sección "Viewing Events in the Web Interface" (Visualización de eventos en la interfaz Web) en la *NetIQ Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

1.5 Catálogo de módulos auxiliares (plug-ins)

Ahora puede ver la lista de módulos auxiliares (plug-ins) instalados en el servidor Sentinel. En la interfaz **Módulos auxiliares (plug-ins)** > **Catálogo** se ofrece una lista de todos los recopiladores, conectores, acciones, integradores y datos instalados en su servidor Sentinel. También puede ver la versión, la fecha de lanzamiento y otros metadatos de los módulos auxiliares (plug-ins), que le ayudan a determinar si tiene la versión más reciente de un módulo auxiliar. Para ver la lista de módulos auxiliares (plug-ins), debe tener la función del administrador.

1.6 Dispositivo en formato OVF

Ahora Sentinel proporciona dispositivos en formato Open Virtual Machine (OVF), lo cual elimina la necesidad de tener diferentes formatos de dispositivo para cada software de virtualización. El dispositivo OVF de Sentinel reemplaza a los de VMware y Xen. Puede utilizar el dispositivo OVF para instalar Sentinel en las plataformas de virtualización de VMware y Citrix Xen. Las actualizaciones del dispositivo en el canal NCC seguirán actualizando los dispositivos existentes en los formatos de Xen o VMware. Para obtener más información sobre cómo instalar el dispositivo Sentinel en formato OVF, consulte la sección "Installing OVF Appliance" (Instalación del dispositivo OVF) en la *NetIQ Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de NetIQ Sentinel).

1.7 Mejoras en la configuración multiarrendatario

Sentinel 7.3 incluye varias mejoras en la configuración multiarrendatario para proveedores de servicios de seguridad gestionados (MSSP):

- **Capacidad para gestionar arrendatarios:** está disponible una nueva interfaz de usuario que le permite crear arrendatarios antes de recibir datos del arrendatario en cuestión. Esta interfaz de usuario también le permite habilitar e inhabilitar arrendatarios.
- **Funciones y usuarios específicos del arrendatario:** cuando cree funciones, puede asignar una función al arrendatario por defecto o a un arrendatario determinado. El arrendatario por defecto proporciona acceso a datos de todos los arrendatarios. Puede utilizar el arrendatario por

defecto en entornos sin arrendatarios y para usuarios de MSSP que necesiten acceso a datos de todos los arrendatarios. Los usuarios de una función asignada a un arrendatario específico solo pueden ver los datos etiquetados con el nombre de dicho arrendatario. Los empleados de MSSP que necesiten ver los datos de varios arrendatarios se pueden asignar al arrendatario por defecto, que les otorgará acceso a datos y vistas en tiempo real de todos los arrendatarios.

Para obtener información detallada acerca de estas mejoras y la configuración multiarrendatario, consulte la sección "Configuring Sentinel in Multi-Tenancy Environments" (Configuración de Sentinel en entornos multiarrendatario) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

1.8 Mejoras en los eventos correlacionados

Sentinel 7.3 incluye las siguientes mejoras en eventos correlacionados:

- **Capacidad para personalizar el evento correlacionado:** ahora la interfaz **Correlación** incluye una opción que le permite personalizar los valores del campo de evento correlacionado al crear la regla de correlación. Por ejemplo, si no quiere que un evento correlacionado tenga la misma gravedad que los eventos activadores, puede ajustar la gravedad en un valor nuevo. Para obtener más información, consulte la sección "Customizing Correlated Event" (Personalización de un evento correlacionado) en la *NetIQ Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).
- **Capacidad para configurar el número de eventos activadores:** ahora puede definir el número de eventos activadores que se pueden asociar con una regla de correlación. Si se define este límite, se impide que Sentinel asocie un número elevado de eventos activadores al evento correlacionado y, de este modo, se reduce la carga en el servidor. Para·obtener·más·información,·consulte·la·sección·"Configuring·the·Number·of·Trigger·Events·to·Associate·with·a·Correlated·Event"(Configuración del·número·de·eventos·activadores·que·se·asocian·a·un·evento·correlacionado)·en·la·*NetIQ·Sentinel·Administration·Guide*·(Guía de administración de NetIQ Sentinel).

1.9 Mejoras en las consolas de inteligencia de seguridad

Sentinel 7.3 incluye las siguientes mejoras en las consolas de inteligencia de seguridad:

- **Capacidad para incluir datos históricos:** ahora puede incluir datos históricos cuando llene la consola con los datos de inteligencia de seguridad, lo cual proporciona más contexto al analizar los datos.
- **Más períodos de retención de datos:** ahora puede conservar datos de inteligencia de seguridad hasta durante 64 semanas.

Para obtener más información, consulte "Creating a Dashboard" (Creación de consolas) en la *NetIQ Sentinel User Guide* (Guía del usuario de NetIQ Sentinel).

1.10 Cambios de terminología para la configuración de múltiples instancias (distribuida)

Sentinel 7.3 cambia la terminología utilizada en la interfaz de usuario de configuración de múltiples instancias (distribuida). Estos cambios muestran que la configuración de múltiples instancias está diseñada para la federación de datos, y no es específica para la búsqueda de eventos. A continuación se indican los cambios de terminología:

- La búsqueda distribuida es ahora federación de datos.
- Los destinos son ahora orígenes de datos.

* El servidor de destino de búsqueda es ahora el servidor de origen de datos.
* El servidor iniciador de búsqueda es ahora el solicitante autorizado.

Para obtener más información, consulte la sección "Configuring Data Federation" (Configuración de la federación de datos) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

1.11 Mejoras en las licencias de Sentinel

La licencia de prueba por defecto para nuevas instalaciones de Sentinel le permite utilizar todas las funciones de Sentinel Enterprise durante un período de evaluación de 60 días, con un EPS ilimitado. Cuando caduca la licencia de prueba, el sistema se ejecuta con una clave de licencia gratuita que admite un conjunto limitado de funciones y un número de eventos limitado de 25 EPS. La licencia gratuita no caduca nunca.
Para·obtener·más·información·acerca·de·las·licencias·de·Sentinel,·consulte·la·sección·"Understanding·License·Information·"(Información·de·licencia)·de·la·*NetIQ·Installation·and·Configuration·Guide· (Guía de instalación y configuración de NetIQ).*

1.12 Capacidad para cambiar el tamaño de la ventana Propiedades de la lista dinámica

Ahora puede cambiar el tamaño de la ventana Propiedades de la lista dinámica, lo cual facilita la visualización de valores largos.

1.13 Eliminación automática de informes antiguos

Sentinel elimina automáticamente los informes antiguos para optimizar la utilización del espacio de disco. Puede definir el período de retención de informes que desee. Para obtener más información, consulte la sección "Configuring the Report Retention Period" (Configuración del período de retención de informes) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

1.14 Módulos auxiliares (plug-ins) más recientes

Sentinel 7.3 incluye versiones nuevas y actualizadas de los módulos auxiliares (plug-ins) de Sentinel. La versión más reciente de los recopiladores y conectores está disponible solamente cuando se realiza una nueva instalación. Las versiones más recientes de integradores y acciones están disponibles tanto en nuevas instalaciones como en actualizaciones. Para obtener instalaciones de actualización de Sentinel 7.3, puede visitar el sitio Web de módulos auxiliares (plug-ins) de Sentinel, consultar el historial de revisiones de los recopiladores y conectores más recientes en la documentación específica y después determinar qué módulos auxiliares (plug-ins) le conviene descargar e instalar.

1.15 Correcciones de software

Sentinel 7.3 incluye correcciones de software que solucionan varios problemas.

Para conocer la lista de correcciones y mejoras de software de versiones anteriores, consulte las notas de la versión específicas.

1.15.1 No es posible exportar resultados de búsqueda con más de 50 000 eventos

Problema: No se pueden exportar a un archivo los resultados de búsquedas distribuidas que tengan más de 50 000 eventos. (`ERROR 863985`)

Solución: Ahora puede exportar archivos de resultados de búsqueda que contengan hasta 200 000 eventos.

1.15.2 El tamaño del buffer de datos en bruto tiene un límite fijo para almacenar datos entrantes

Problema: El tamaño del buffer de datos en bruto tiene un límite fijo para almacenar datos en bruto entrantes. Si la cantidad de datos entrantes supera este límite, Sentinel descarta los datos en bruto aunque haya suficiente espacio de disco. (`ERROR 893546`)

Solución: No hay ningún límite de tamaño para el buffer de datos en bruto. Sentinel puede almacenar en buffer datos en bruto hasta que el disco esté un 90 % lleno.

1.15.3 No es posible volver a implantar una regla de correlación si hay varias pestañas de reglas abiertas

Problema: No es posible volver a implantar reglas de correlación si hay varias pestañas de reglas abiertas al mismo tiempo. (`ERROR 838771`)

Solución: Ahora puede volver a implantar reglas de correlación aunque haya varias pestañas de reglas abiertas al mismo tiempo.

1.15.4 Hay que pulsar la tecla Intro dos veces al buscar un evento

Problema: Cuando busca un evento, si edita la consulta de búsqueda, tiene que pulsar Intro o **Buscar** dos veces para iniciar la búsqueda.(`ERROR 829291`)

Solución: La búsqueda del evento empieza cuando se pulsa Intro o **Buscar** una vez después de editar una consulta de búsqueda.

1.15.5 No es posible ver la información del evento Change Guardian sin la clave de licencia de Change Guardian

Problema: Sentinel solicita la licencia de Change Guardian cuando se hace clic en el icono de Change Guardian para ver la información del evento. (`ERROR 855914`)

Solución: Ahora puede ver la información del evento Change Guardian sin necesidad de añadir la clave de licencia de dicho evento.

1.15.6 El instalador de actualización de dispositivos elimina las reglas de cortafuegos personalizadas durante la actualización

Problema: Sentinel elimina las reglas de cortafuegos personalizadas durante la actualización de dispositivos Sentinel. (`ERROR 867662`)

Solución: Sentinel 7.3 conserva las reglas de cortafuegos personalizadas actuales.

1.15.7 Errores al procesar datos en bruto

Problema: Sentinel no procesa los archivos de datos en bruto que no se cerraron correctamente. Este problema es esporádico.(`ERROR 870969`)

Solución: Ahora Sentinel 7.3 procesa los archivos de datos en bruto que no se cerraron correctamente.

1.15.8 El filtro de atributos de la vista Gestión de orígenes de eventos no expande automáticamente los orígenes de eventos

Problema: En la vista de tabla Gestión de orígenes de eventos, al filtrar por atributos se muestra una vista contraída de los orígenes de eventos. Debe expandir la vista manualmente. (`ERROR 790041`)

Solución: En Sentinel 7.3, la vista Gestión de orígenes de eventos se expande automáticamente cuando se filtra por atributos.

1.15.9 Sentinel no muestra los adjuntos del evento Change Guardian tras una visualización

Problema: Sentinel no muestra los adjuntos del evento Change Guardian cuando los ha visualizado una vez. Solo muestra los adjuntos del evento correctamente la primera vez. (`ERROR 902142`)

Solución: Sentinel 7.3 muestra los adjuntos del evento Change Guardian correctamente.

1.15.10 La sincronización de bases de datos entre Sentinel y Sentinel Agent Manager no es fiable

Problema: Las actividades que realice en Sentinel Agent Manager (SAM), como autorizar a un agente, no siempre se sincronizan en Sentinel. Este problema se debe a un error en el guion ETL que se utiliza para sincronizar las bases de datos de SAM y Sentinel. (`ERROR 885456`)

Solución: En Sentinel 7.3, la sincronización entre las bases de datos de SAM y de Sentinel se realiza correctamente. Las tareas realizadas en SAM se sincronizan en Sentinel en unos minutos.

1.15.11 Los campos de eventos geoespaciales no se llenan con los datos correctos

Problema: Los campos de eventos geoespaciales Latitud, Longitud y País para los hosts de origen, destino y observador están mal ajustados.(`ERROR 895872`)

Solución: Ahora Sentinel llena los campos de evento Latitud y Longitud con valores correctos. Ahora los campos de evento País se llenan con el código ISO de país de dos caracteres, en vez de con el nombre completo del país, de modo que son compatibles con más configuraciones regionales y herramientas de visualización.

1.15.12 El guion clean_db.sh no elimina los datos del asesor en las instalaciones personalizadas

Problema: El guion `clean_db.sh` no elimina los datos del asesor en las instalaciones personalizadas, donde estos datos están presentes en ubicaciones diferentes a las ubicaciones por defecto.(`ERROR 820700`)

Solución: Ahora el guion `clean_db.sh` elimina los datos del asesor de la ubicación por defecto y de las demás.

1.15.13 Problemas de conexión entre clientes y Sentinel en modo FIPS

Problema: Las versiones anteriores de Sentinel incluyen la actualización 65 de Oracle Java 1.7, que presenta un problema conocido relacionado con el intercambio de claves del cliente RSA en modo FIPS. Para obtener más información, consulte las notas de la versión del kit SDK de Java SE 7.51. Esto provoca problemas de conexión cuando Sentinel se ejecuta en modo FIPS e intenta recibir conexiones de clientes como Security Manager y Sentinel Agent Manager. (`ERROR 872305`)

Solución: Sentinel 7.3 incluye la actualización 72 de Oracle Java 1.7, que soluciona el problema con el intercambio de claves de RSA.

1.15.14 La búsqueda de eventos no funciona tras el fallo de una búsqueda distribuida

Problema: Sentinel no devuelve ningún resultado cuando se realiza una búsqueda de evento después de que haya fallado una búsqueda distribuida. La búsqueda de eventos deja de funcionar y no se puede realizar ninguna otra búsqueda. (`ERROR 864372`)

Solución: Ahora Sentinel cierra las tareas de búsqueda que están esperando datos después de un error de búsqueda y permite realizar nuevas búsquedas.

2 Requisitos del sistema

Para obtener más información sobre los requisitos de hardware, los sistemas operativos compatibles y los navegadores, consulte la sección "Meeting System requirements" (Cumplimiento de los requisitos del sistema) de la *NetIQ Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de NetIQ Sentinel).

3 Instalación de Sentinel 7.3

Para obtener información acerca de la instalación de Sentinel 7.3, consulte la *NetIQ Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de NetIQ Sentinel).

4 Actualización a Sentinel 7.3

La actualización a Sentinel 7.3 puede realizarse desde Sentinel 7.0 o versiones posteriores.

Descargue el instalador de Sentinel del sitio Web de descargas de NetIQ. Para obtener más información sobre la actualización a Sentinel 7.3, consulte la sección "Upgrading Sentinel" (Actualización de Sentinel) en la *NetIQ Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de NetIQ Sentinel).

4.1 Configuración posterior a la actualización

Tras la actualización, la función Usuario apoderado de datos no tendrá el permiso **Permitir a los usuarios gestionar las alertas**. Este permiso es necesario para que la función pueda realizar la búsqueda de alertas remotas. Asigne manualmente el permiso **Permitir a los usuarios gestionar las alertas** a la función Usuario apoderados de datos. Para obtener más información, consulte la sección "Configuring Roles and Users" (Configuración de funciones y usuarios) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

5 Problemas conocidos

NetIQ Corporation se esfuerza por garantizar que nuestros productos ofrezcan soluciones de calidad para sus necesidades de software empresarial. Se están investigando los siguientes asuntos. Si necesita más ayuda con algún problema, póngase en contacto con el departamento de Asistencia técnica.

5.1 El proveedor del rastreador SpyEye ha interrumpido la alimentación de datos

Problema: El proveedor de datos del rastreador SpyEye ha interrumpido las actualizaciones de estos datos, con el argumento de que la amenaza de SpyEye parece haberse mitigado. El módulo auxiliar (plug-in) de alimentación sigue formando parte del paquete de Sentinel. Dado que el proveedor de datos ya no proporciona datos de amenazas válidos, este módulo auxiliar (plug-in) llena las listas dinámicas con datos inesperados y las reglas de correlación relacionadas no funcionan correctamente. La interfaz de usuario de Datos solo indica que los datos se procesaron correctamente, pero no que no son válidos. `(ERROR 916560)`.

Solución: El módulo auxiliar (plug-in) del rastreador de SpyEye no provoca problemas en su servidor, pero puede ahorrar recursos del sistema si elimina tanto el módulo como los objetos de Sentinel relacionados: la lista dinámica y las reglas de correlación.

Desinstale el componente botnet de SpyEye en el Gestor de paquetes de soluciones. Al hacerlo, se eliminarán las listas dinámicas, las reglas de correlación y el módulo auxiliar (plug-in) Datos asociados. No obstante, si el módulo auxiliar (plug-in) Datos se programó o ejecutó previamente, no podrá eliminarlo. En su lugar, puede ajustar la programación de actualización de los datos en Nunca. Para obtener más información acerca de cómo eliminar el componente botnet de SpyEye en el Gestor de paquetes de soluciones, consulte la documentación del Threat Intelligence Solution Pack en el sitio Web de módulos auxiliares (plug-ins) de Sentinel.

5.2 La búsqueda en la tabla Sugerencias no devuelve la lista completa de campos de alerta en las instalaciones actualizadas de Sentinel

Problema: En las instalaciones actualizadas de Sentinel 7.3, cuando se buscan atributos de alerta en la tabla Sugerencias de la consola Web, la búsqueda no devuelve la lista completa de campos de alerta. Sin embargo, los campos de alerta se muestran correctamente en la tabla Sugerencias al borrar la búsqueda.`(ERROR 914755)`

Solución: No existe ninguna solución por el momento.

5.3 No es posible lanzar el Centro de control de Sentinel y Solution Designer con JRE 8 cuando Sentinel se encuentra en modo FIPS

Problema: Cuando el servidor Sentinel se ejecuta en modo FIPS 140-2, no es posible lanzar el Centro de control de Sentinel ni Solution Designer en el equipo cliente mediante Java Web Start con la versión 8 de Java Runtime Environment (JRE) o una posterior. `(ERROR 910452)`

Solución: Asegúrese de que hace lo siguiente en el equipo cliente donde desea lanzar el Centro de control de Sentinel o Solution Designer:

- Instale y use JRE 7 para lanzar el Centro de control de Sentinel o Solution Designer.
- En el panel de control de Java, no seleccione la opción **Usar TLS 1.2** en la pestaña **Avanzado**.

5.4 La sincronización de datos falla al sincronizar direcciones IPv6 en un formato legible para el ser humano

Problema: La sincronización de datos falla cuando intenta sincronizar campos de dirección IPv6 en un formato legible para el ser humano con bases de datos externas. Para obtener más información acerca de cómo configurar Sentinel para llenar los campos de dirección IP en un formato de notación con punto legible para el ser humano, consulte la sección "Creating a Data Synchronization Policy" (Creación de una directiva de sincronización de datos) de la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel). `(ERROR 913014)`

Solución: Para solucionar este problema, cambie manualmente el tamaño máximo de los campos de dirección IP a al menos 46 caracteres en la base de datos de destino y vuelva a sincronizar la base de datos.

5.5 La búsqueda de eventos no responde si no dispone de permisos para ver eventos

Problema: Si ejecuta una búsqueda de evento cuando no tiene seleccionado ningún filtro de seguridad para su función y dicha función no tiene permisos para ver eventos, la búsqueda no se llevará a cabo. La búsqueda no muestra ningún mensaje de error acerca de los permisos para ver eventos no válidos. `(ERROR 908666)`

Solución: Actualice la función con una de las opciones siguientes:

1. Especifique un criterio en el campo **Solo eventos que coinciden con los criterios**. Si los usuarios de la función no deben ver ningún evento, puede introducir **NOT sev:[0 TO 5]**.
2. Seleccione **Ver eventos del sistema**.
3. Seleccione **Ver todos los datos de eventos (incluidos los datos en bruto y los datos de NetFlow)**.

5.6 Sentinel Agent Manager no tiene en cuenta la configuración de RawDataTapFileSize

Problema: Sentinel Agent Manager ignora el valor especificado en el atributo `RawDataTapFileSize` del archivo `SMServiceHost.exe.config` para la configuración del tamaño de archivo de datos en bruto, y deja de escribir en el archivo de datos en bruto cuando su tamaño alcanza los 10 MB.`(ERROR 867954)`

Solución: Copie el contenido del archivo de datos en bruto en otro archivo de forma manual y bórrelo cuando su tamaño alcance los 10 MB, de modo que Sentinel Agent Manager pueda escribir datos nuevos en él.

5.7 Falta el panel Campos de evento en la página Programación cuando se editan algunas búsquedas guardas

Problema: Cuando se edita una búsqueda guardada que se actualizó de Sentinel 7.2 a una versión posterior, la página Programación no muestra el panel **Campos de evento**, usado para especificar campos de salida en el archivo CSV de informe de la búsqueda. `(ERROR 900293)`

Solución: Después de actualizar Sentinel, vuelva a crear y programar la búsqueda para ver el panel **Campos de evento** en la página Programación.

5.8 Sentinel no devuelve ningún evento correlacionado cuando se buscan eventos para la regla implantada con la búsqueda de número de activaciones por defecto

Problema: Sentinel no devuelve ningún evento correlacionado cuando se buscan todos los eventos correlacionados que se generaron después de implantar o habilitar la regla, haciendo clic en el icono situado junto a **Número de activaciones** en el panel **Estadísticas de actividad** de la página de resumen de correlaciones para dicha regla. `(ERROR 912820)`

Solución: Cambie el valor del campo **Desde** en la página de búsqueda de eventos por una hora anterior a la que se muestra en el campo y vuelva a hacer clic en **Buscar**.

5.9 En modo FIPS Sentinel no muestra la información adjunta de cambios en Change Guardian

Problema: En modo FIPS, Sentinel no muestra la información adjunta de cambios en Change Guardian cuando se buscan eventos de Change Guardian y se hace clic en el icono de **Change Guardian**, en vez de estar configurado para recibir eventos de Change Guardian. La versión 4.1.1.1 de Change Guardian, y las versiones anteriores, no permiten el envío de eventos en modo compatible con FIPS.`(ERROR 912230)`

Solución: No existe ninguna solución por el momento.

5.10 El número de ocurrencias disminuye al actualizar la vista de alertas

Problema: En la vista de alertas, el número de **ocurrencias** disminuye cuando se actualiza la vista de alertas.(ERROR 913838)

Solución: Haga clic en **Ver detalles**, junto a la alerta para la que haya disminuido el número de **ocurrencias**, para acceder a la página Resumen de la alerta. La página Resumen de la alerta muestra el valor correcto de **Ocurrencias**.

5.11 La recopilación y sincronización de datos con la base de datos DB2 fallan tras la actualización a Sentinel 7.3

Problema: La actualización a Sentinel 7.3 provoca el fallo de la recopilación y sincronización de datos con la base de datos DB2, ya que elimina el controlador IBM DB2 JDBC.(ERROR 909343)

Solución: Después de actualizar a Sentinel 7.3, añada el controlador JDBC correcto y configúrelo para la recopilación y sincronización de datos. Siga estos pasos para hacerlo:

1. Copie la versión correcta del controlador IBM DB2 JDBC (`db2jcc-*.jar`) para su versión de base de datos DB2 en la carpeta `/opt/novell/sentinel/lib`.
2. Asegúrese de definir la propiedad y los permisos necesarios para el archivo de controlador.
3. Configure este controlador para la recopilación de datos. Para obtener más información, consulte la documentación del conector de base de datos.

5.12 Las nuevas alertas entrantes se muestran incorrectamente como seleccionadas al modificar las alertas existentes

Problema: Cuando hace clic en **Seleccionar todo** en las vistas de alertas para seleccionar alertas, deselecciona algunas alertas y las modifica, las nuevas alertas entrantes también se seleccionan en las vistas de alertas actualizadas. En consecuencia, el número de alertas seleccionadas para su modificación es incorrecto y parece como si también fuese a modificar las nuevas alertas entrantes. No obstante, solo se modifican las alertas seleccionadas en un principio.(ERROR 904830)

Solución: No se mostrará ninguna alerta nueva en la vista de alertas si crea esta vista con un rango de tiempo personalizado.

5.13 La carga de datos históricos de inteligencia de seguridad es muy lenta

Problema: Los datos históricos de inteligencia de seguridad (IS) tardan mucho en cargarse en sistemas de Sentinel que presentan una carga elevada de eventos por segundo (EPS). (ERROR 908599)

Solución: Si va a crear una consola de inteligencia de seguridad con datos históricos, planifique la implantación de la consola cuando la carga del sistema sea menor, si es posible. No existe ninguna otra solución por el momento.

5.14 La consola de inteligencia de seguridad muestra una duración de línea de base no válida al regenerar una línea de base

Problema: Durante la regeneración de la línea de base de inteligencia de seguridad, las fechas de inicio y fin de la línea de base son incorrectas y se muestra 1/1/1970.(ERROR 912009)

Solución: Las fechas correctas se actualizan al finalizar la regeneración de la línea de base.

5.15 El servidor Sentinel se apaga al ejecutar una búsqueda si hay muchos eventos en una sola partición

Problema: El servidor Sentinel se apaga al ejecutar una búsqueda si hay muchos eventos indexados en una sola partición. (ERROR 913599)

Solución: Cree directivas de retención de modo que haya al menos dos particiones abiertas en un día. El hecho de tener más de una partición abierta contribuye a reducir el número de eventos indexados en las particiones.

Puede crear directivas de retención que filtren los eventos en función del campo `estzhour`, que rastrea la hora del día. Por lo tanto, puede crear una directiva de retención con el filtro `estzhour:[0 TO 11]` y otra con el filtro `estzhour:[12 TO 23]`.

Para obtener más información, consulte "Configuring Data Retention Policies" (Configuración de directivas de retención de datos) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

5.16 A veces la transferencia ascendente de alertas falla y se crea una alerta nueva

Problema: Se crea una alerta nueva en vez de transferirse la información de la alerta a una alerta existente. Este problema es esporádico. (ERROR 914512)

Solución: No existe ninguna solución por el momento.

5.17 Error al utilizar el guion report_dev_setup.sh para configurar los puertos de Sentinel para excepciones de cortafuegos en las instalaciones actualizadas de dispositivos Sentinel

Problema: Sentinel muestra un error cuando se utiliza el guion `report_dev_setup.sh` para configurar los puertos de Sentinel para excepciones de cortafuegos. (ERROR 914874)

Solución: Siga estos pasos para configurar los puertos de Sentinel para excepciones de cortafuegos:

1. Abra el archivo `/etc/sysconfig/SuSEfirewall2`.
2. Cambie la línea siguiente:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   a

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Reinicie Sentinel.

5.18 El rendimiento del recopilador genérico de Sentinel se deteriora cuando se habilita el recopilador genérico de servicios de resolución de nombres de host

Problema: El rendimiento del recopilador genérico de Sentinel se deteriora cuando se habilita el recopilador genérico de servicios de resolución de nombres de host en Microsoft Active Directory y Windows Collector. El EPS se reduce en un 50% cuando los gestores de recopiladores remotos envían eventos. (ERROR 906715)

Solución: No existe ninguna solución por el momento.

5.19 Sentinel no puede acceder a datos de Inteligencia de seguridad, Netflow y Alertas en el modo FIPS

Problema: Cuando se instala Sentinel en modo FIPS, el conector para la base de datos de Inteligencia de seguridad no se inicia y Sentinel no puede acceder a los datos de Inteligencia de seguridad, Netflow y Alertas. (ERROR 915241)

Solución: Reinicie Sentinel tras la instalación y configuración en modo FIPS.

5.20 A veces la base de datos de Inteligencia de seguridad y la consola de alertas no funcionan en instalaciones personalizadas actualizadas de Sentinel con FIPS habilitado

Problema: Cuando se actualiza a Sentinel 7.3 desde una instalación personalizada de Sentinel que instaló un usuario diferente a root y se configuró en modo FIPS, a veces la base de datos de Inteligencia de seguridad y la consola de alertas no se inician. (ERROR 916285)

Solución: Realice los siguientes pasos:

1. Vaya a <*directorio de instalación personalizada*>/opt/novell/sentinel/bin para conocer el servicio de indexado de Sentinel.
2. Ejecute el comando siguiente:

   ```
   ./si_db.sh status
   ```

   Verifique si se muestra la siguiente salida:

   ```
   Connection between alert store and indexing service is running.
   Security Intelligence database is running.
   Indexing service is running.
   ```

   Si alguno de estos tres servicios no se está ejecutando, realice los pasos siguientes.
3. Ejecute el siguiente comando para detener Sentinel:

   ```
   rcsentinel stop
   ```
4. Entre en el servidor Sentinel como el usuario novell.
5. Ejecute el comando siguiente:

   ```
   <directorio de instalación personalizado>/opt/novell/sentinel/bin/si_db.sh
   startnoauth
   ```
6. Ejecute los comandos siguientes para añadir los usuarios dbauser y appuser:

   ```
   cd <directorio de instalación personalizado>/opt/novell/sentinel/3rdparty/
   mongodb/bin
   ```

```
./mongo
use admin
db.addUser ("dbauser", "novell")
use analytics
db.addUser ("appuser", "novell")
exit
```

7 Detenga la base de datos MongoDB:

```
<directorio de instalación personalizado>/opt/novell/sentinel/bin/si_db.sh
stop
```

8 Efectúe estos pasos para añadir campos de contraseña cifrada:

8a Ejecute el comando siguiente para obtener la contraseña cifrada para el usuario novell:

```
<directorio de instalación personalizada>/opt/novell/sentinel/bin/
encryptpwd -e novell
```

Se muestra la contraseña cifrada. Por ejemplo:

```
bVWOzu6okMmMCkgM0aHeQ==
```

8b En el archivo `configuration.properties`, actualice las propiedades `baselining.sidb.password` y `baselining.sidb.dbpassword` con la contraseña cifrada. por ejemplo:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

9 Cierre la cuenta de usuario novell e inicie Sentinel como usuario root con el comando siguiente:

```
rcsentinel start
```

Nota: Ejecute el guion `configure.sh` para restablecer la contraseña cuando sea necesario. Para obtener más información acerca de cómo ejecutar el guion `configure.sh`, consulte la sección "Modifying the Configuration after Installation" (Modificación de la configuración tras la instalación) de la *NetIQ Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de NetIQ Sentinel).

5.21 Sentinel no muestra eventos activadores para alertas remotas

Problema: En las vistas de alertas, cuando hace clic en **Ver detalles** junto a una alerta remota y va a la página Información de alerta, los eventos activadores para dicha alerta no se muestran en el panel **Datos asociados.**`(ERROR 916116)`

Solución: Entre al servidor de origen de datos y vea la información de la alerta localmente.

5.22 Sentinel no muestra las propiedades de alertas personalizadas en las vistas de alertas remotas

Problema: En las vistas de alertas, los campos **Estado** y **Prioridad** de las alertas remotas no muestran datos si sus valores están personalizados. Puede que estos campos tampoco muestren datos en la página Información de alerta de las alertas. `(ERROR 915762)`

Solución: Entre al servidor de origen de datos y vea las alertas localmente.

5.23 A veces Sentinel no muestra alertas en las vistas de alertas después de un reinicio

Problema: A veces Sentinel no muestra alertas en ninguna vista de alertas si el usuario reinicia y vuelve a entrar a Sentinel.(ERROR 916133)

Solución: Efectúe estos pasos para reiniciar la base de datos de Inteligencia de seguridad:

1 Ejecute el comando siguiente:

```
rm /opt/novell/sentinel/3rdparty/mongoconnector/config.txt
```

2 Edite /opt/novell/sentinel/bin/elasticsearch.sh de la siguiente manera:

2a En function es_start(), introduzca sleep 2 después del número de línea 209, tal como se muestra en este fragmento de código:

```
 exec_command "\"${ESEC_HOME}/3rdparty/elasticsearch/bin/elasticsearch\" -
d -Des.config.file=\"${ESEC_CONFIG_HOME}/3rdparty/elasticsearch/
elasticsearch.yml\" -Des.path.conf=\"${ESEC_CONFIG_HOME}/3rdparty/
elasticsearch\" -Des.path.data=\"${ESEC_DATA_HOME}/3rdparty/elasticsearch/
data\" -Des.path.logs=\"${ESEC_LOG_HOME}/log\""
                if [ $? -ne 0 ]
                then
                        RETRY=$(( $RETRY + 1 ))
                        error_message "$(gettext 'Failed to start indexing
service.')"
                        if [ $RETRY -eq 5 ]
                        then
                        return $RESULT_FAILURE
                        fi
                        sleep 2
                        continue
                fi
                sleep 2
       fi
```

2b Guarde el archivo y cierre el editor.

3 Ejecute el comando siguiente como usuario novell:

```
/opt/novell/sentinel/bin/si_db.sh restart
```

5.24 Faltan usuarios en la base de datos de Inteligencia de seguridad en las instalaciones de dispositivos Sentinel actualizadas

Problema: En las instalaciones en línea de los dispositivos Sentinel actualizados, las cuentas de usuario appuser y dbauser no están disponibles. (ERROR 915197)

Solución: Realice los siguientes pasos:

1 Detenga los servicios de Sentinel:

```
rcsentinel stop
```

2 Ejecute el comando siguiente:

```
/opt/novell/sentinel/bin/si_db.sh startnoauth
```

3 Ejecute los comandos siguientes para añadir los usuarios dbauser y appuser:

```
cd opt/novell/sentinel/3rdparty/mongodb/bin

./mongo

use admin

db.addUser ("dbauser", "novell")
```

```
use analytics
db.addUser ("appuser", "novell")
exit
```

4 Ejecute el comando siguiente:

```
/opt/novell/sentinel/bin/si_db.sh stop
```

5 Efectúe estos pasos para añadir campos de contraseña cifrada:

5a Ejecute el comando siguiente para obtener la contraseña cifrada para el usuario novell:

```
/opt/novell/sentinel/bin/encryptpwd -e novell
```

Se muestra la contraseña cifrada. Por ejemplo:

```
bVWOzu6okMmMCkgM0aHeQ==
```

5b En el archivo `configuration.properties`, actualice las propiedades `baselining.sidb.password` y `baselining.sidb.dbpassword` con la contraseña cifrada. por ejemplo:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

6 Cierre la cuenta de usuario novell e inicie Sentinel como usuario root con el comando siguiente:

```
rcsentinel start
```

5.25 Vulnerabilidad de la seguridad en SSL 3.0

Problema: SSL 3.0 presenta una vulnerabilidad que puede permitir el cálculo del texto sin cifrar en conexiones seguras. Para obtener más información, consulte el sitio CVE-2014-3566. Esta vulnerabilidad existe en la versión incluida en el conector de Syslog 2011.1r4 porque utiliza el protocolo SSL.

Solución: Este problema se ha solucionado en la versión 2011.1r5 del conector de Syslog y en las versiones posteriores. Mientras no se publique oficialmente en el sitio Web de módulos auxiliares (plug-ins) de Sentinel, puede descargar el conector en la sección de vistas previas.

5.26 Agent Manager Connector no ajusta la propiedad Modo de conexión de los eventos si el recopilador asociado admite varios modos de conexión

Problema: La versión 2011.1r3 de Agent Manager Connector no ajusta la propiedad CONNECTION_MODE de los eventos si el recopilador que analiza los eventos admite varios modos de conexión. (`ERROR 880564`)

Solución: Este problema se ha solucionado en la versión 2011.1r5 de Agent Manager Connector y en las versiones posteriores. Mientras no se publique oficialmente en el sitio Web de módulos auxiliares (plug-ins) de Sentinel, puede descargar el conector en la sección de vistas previas.

5.27 Sentinel no configura la interfaz de red de la aplicación Sentinel por defecto

Problema: Cuando se instala la aplicación Sentinel, la interfaz de red no está configurada por defecto. (`ERROR 867013`)

Solución: Para configurar la interfaz de red:

1. En la página Configuración de red, haga clic en **Interfaces de red**.
2. Seleccione la interfaz de red y haga clic en **Editar**.
3. Seleccione **Dirección dinámica** y, a continuación, seleccione **DHCP** o **Dirección IP estática asignada**.
4. Haga clic en **Siguiente** y, a continuación, en **Aceptar**.

5.28 El navegador Web muestra un error al exportar los resultados de la búsqueda en Sentinel

Problema: Cuando se exportan los resultados de la búsqueda en Sentinel, es posible que el navegador Web muestre un error si se modifican los ajustes de idioma del sistema operativo. (`ERROR 834874`)

Solución: Para exportar los resultados de la búsqueda correctamente, realice una de las siguientes operaciones:

- Durante la exportación, elimine los caracteres especiales (que no sean ASCII) del nombre de archivo de exportación.
- Habilite UTF-8 en los ajustes de idioma del sistema operativo, reinicie el equipo y, a continuación, reinicie el servidor Sentinel.

5.29 Al lanzar la consola Web de Sentinel con redirección de puertos o conversión de direcciones de red de destino se muestra una página en blanco

Problema: Cuando se lanza la consola Web de Sentinel con las opciones de redirección de puertos o conversión de direcciones de red de destino (DNAT), esta muestra una página en blanco. (`ERROR 694732`)

Solución: No utilice la redirección de puertos o la conversión de direcciones de red de destino (DNAT) para lanzar la consola Web de Sentinel.

5.30 Sentinel podría mostrar un error cuando se crea o regenera una línea de base

Problema: Cuando se crea o regenera una línea de base de inteligencia de seguridad, Sentinel crear la línea de base correctamente, pero muestra un mensaje de error. (`ERROR 848067`)

Solución: Haga caso omiso de este mensaje de error. La creación de la línea de base puede tardar varios minutos.

5.31 Las particiones eliminadas del almacenamiento secundario también se eliminan del almacenamiento principal

Problema: Si el número de días de datos que puede retener el almacenamiento secundario es inferior al número de días que retiene el almacenamiento principal, Sentinel no usa el espacio de disco del almacenamiento principal de forma eficiente. Las particiones eliminadas del almacenamiento secundario para liberar espacio también se eliminarán del almacenamiento principal. (`ERROR 860888`)

Solución: Asigne espacio suficiente en el almacenamiento secundario para retener los datos correspondientes al total de días que desea mantener en línea (que se puedan buscar).

Para obtener más información, consulte la sección "Event Data" (Datos de eventos) en la *NetIQ Sentinel Administration Guide* (Guía de administración de NetIQ Sentinel).

5.32 Es posible que los servicios de Sentinel no se inicien automáticamente tras la instalación

Problema: En sistemas con más de 2 TB de espacio de disco, puede que Sentinel no se inicie automáticamente tras la instalación. (`ERROR 846296`)

Solución: De forma puntual, inicie los servicios de Sentinel manualmente con el comando siguiente:

```
rcsentinel start
```

5.33 No es posible habilitar la autenticación Kerberos en instalaciones de dispositivos Sentinel

Problema: En instalaciones de dispositivos Sentinel, si configura la autenticación Kerberos en el módulo Kerberos, la consola muestra un mensaje para confirmar que el cliente Kerberos se configuró correctamente. Sin embargo, cuando vuelve a ver el módulo Kerberos, la opción **Habilitar autenticación Kerberos** no está seleccionada. (`ERROR 843623`)

Solución: No existe ninguna solución por el momento.

5.34 No es posible instalar el gestor de recopiladores remoto si la contraseña contiene caracteres especiales

Problema: Cuando se instala un gestor de recopiladores remoto, si se especifica una contraseña que contiene caracteres especiales, como $, ", \ o /, la instalación falla y se generan errores. (`ERROR 812111`)

Solución: No utilice caracteres especiales en la contraseña del gestor de recopiladores remoto.

5.35 Al reiniciar el gestor de recopiladores remoto algunos orígenes de eventos pierden la conexión

Problema: Cuando se reinicia un gestor de recopiladores remoto, los orígenes de eventos Syslog conectados al puerto UDP pierden la conexión. (`ERROR 795057`)

Solución: No existe ninguna solución por el momento.

5.36 No es posible ver más de un resultado de informe a la vez

Problema: Mientras espera a que se abra el archivo PDF de resultado de informe, especialmente en el caso de los resultados de informe de 1 millón de eventos, el resultado no se mostrará si hace clic en otro archivo PDF de resultado de informe. (`ERROR 804683`)

Solución: Vuelva a hacer clic en el segundo archivo PDF de resultado de informe para ver el resultado.

5.37 Agent Manager requiere autenticación SQL cuando está habilitado el modo FIPS

Problema: Si tiene el modo FIPS habilitado en su entorno de Sentinel, la autenticación de Windows para Agent Manager provoca el fallo de la sincronización con la base de datos de Agent Manager. (ERROR 814452)

Solución: Utilice la autenticación de SQL para Agent Manager cuando tenga el modo FIPS habilitado en su entorno de Sentinel.

5.38 La instalación de alta disponibilidad de Sentinel en modo FIPS muestra un error

Problema: Si se habilita el modo FIPS, la instalación de alta disponibilidad de Sentinel muestra el error siguiente:

```
El archivo configuration.properties del servidor Sentinel no es correcto. Compruebe
el archivo de configuración y vuelva a ejecutar el guión convert_to_fips.sh para
habilitar el modo FIPS en el servidor Sentinel.
```

No obstante, la instalación finaliza correctamente. (ERROR 817828)

Solución: No existe ninguna solución por el momento. A pesar de que el instalador muestra el error, la configuración de alta disponibilidad de Sentinel funciona correctamente en el modo FIPS.

5.39 La instalación de alta disponibilidad de Sentinel en modo no FIPS muestra un error

Problema: La instalación de alta disponibilidad de Sentinel en modo no FIPS se realiza correctamente, pero muestra el error siguiente dos veces:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

(ERROR 810764)

Solución: No existe ninguna solución por el momento. A pesar de que el instalador muestra el error, la configuración de alta disponibilidad de Sentinel funciona correctamente en el modo no FIPS.

5.40 La actualización del dispositivo de versiones anteriores a Sentinel 7.2 falla en WebYaST

Problema: La actualización de dispositivos de versiones anteriores a Sentinel 7.2 falla porque el proveedor de los paquetes de actualización ha cambiado de Novell a NetIQ. (ERROR 780969)

Solución: Utilice el comando zypper para actualizar la aplicación. Para obtener más información, consulte la sección Upgrading the Appliance by Using zypper (Actualización del dispositivo utilizando zypper) en la *NetIQ Sentinel Installation and Configuration Guide* (Guía de instalación y configuración de NetIQ Sentinel).

5.41 Problema con la entrada a la aplicación Sentinel

Problema: Si especificó un carácter $ en la contraseña, Sentinel almacena la contraseña de una forma diferente en la base de datos dependiendo de dónde se coloca el $ en la contraseña. Si la contraseña empieza con el carácter especial $, Sentinel almacena la contraseña con un nombre de archivo. Si el carácter $ se encuentra en alguna parte hacia la mitad de la contraseña, Sentinel trunca la contraseña en la ubicación del carácter $. (ERROR 734500)

Solución: La contraseña real se almacena en el archivo `home/novell/.pgpass`. Obtenga la contraseña de este archivo y luego entre en Sentinel. Por ejemplo, si especificó la contraseña como abc$123, Sentinel almacena la contraseña como abc en el archivo `.pgpass`. Puede entrar en Sentinel especificando abc como contraseña.

5.42 Error al instalar reglas de correlación

Problema: Solution Manager no instala las reglas de correlación cuando ya existe en el sistema una regla de correlación con nombre idéntico. Se registra un error `NullPointerException` en la consola. (ERROR 713962)

Solución: Asegúrese de que todas las reglas de correlación tengan un nombre exclusivo.

5.43 La acción de Sentinel Link muestra un mensaje incorrecto

Problema: Al ejecutar una acción de Sentinel Link desde la consola Web de Sentinel, Sentinel muestra un mensaje de acción correcta incluso cuando la prueba de integración del conector de Sentinel Link ha fallado en el Centro de control de Sentinel. (ERROR 710305)

Solución: No existe ninguna solución por el momento.

5.44 Consola y definiciones de anomalía con nombres idénticos

Problema: Cuando una consola de Inteligencia de seguridad y una definición de anomalía tienen nombres idénticos, se inhabilita el enlace de la consola en la página de Detalles de anomalía. (ERROR 715986)

Solución: Asegúrese de utilizar nombres exclusivos al crear consolas y definiciones de anomalías.

5.45 Inexactitudes en las columnas Duración y Accedido de las tareas de búsqueda activas

Problema: La consola Web de Sentinel muestra números negativos en las columnas Accedido y Duración de tareas de búsqueda activas cuando el reloj del ordenador de la consola Web de Sentinel está atrasado con respecto al reloj del servidor Sentinel. Por ejemplo, las columnas Duración y Accedido muestran números negativos cuando el reloj de la consola Web de Sentinel está fijado en la 1:30 PM y el reloj del servidor Sentinel en las 2:30 PM. (ERROR 719875)

Solución: Asegúrese de que la hora en el ordenador que utiliza para acceder a la consola Web de Sentinel sea igual o posterior a la hora del ordenador del servidor Sentinel.

5.46 El evento de auditoría IssueSAMLToken muestra información incorrecta en la consola de inteligencia de seguridad

Problema: Cuando entra a la consola de seguridad y realiza una búsqueda en el evento de auditoría `IssueSAMLToken`, el evento `IssueSAMLToken` muestra un nombre de host (InitiatorUserName) o una IP de origen (dirección IP) incorrectos. `(ERROR 870609)`

Solución: No existe ninguna solución por el momento.

5.47 El Centro de control de Sentinel no se lanza cuando se instala NetIQ Identity Manager Designer en el ordenador cliente

Problema: El Centro de control de Sentinel no se lanza cuando se instala NetIQ Identity Manager Designer en el ordenador cliente y Designer utiliza el JRE del sistema. Designer necesita añadir algunos archivos jar de apoyo como `xml-apis.jar` al directorio `lib/endorsed`. Algunas de las clases del archivo `xml-apis.jar` sustituyen las clases correspondientes del JRE del sistema que utiliza el Centro de control de Sentinel. `(ERROR 888085)`

Solución: Configure Designer para que utilice su propio JRE.

5.48 Sentinel Agent Manager no captura los campos de la cadena de inserción de Windows con valores nulos

Problema: Cuando recopila datos de eventos, Sentinel Agent Manager no captura los campos de la cadena de inserción de Windows que tienen valores nulos. `(ERROR 838825)`

Solución: No existe ninguna solución por el momento.

6 Información de contacto

Nuestro objetivo es proporcionar documentación que satisfaga sus necesidades. Si tiene sugerencias para mejorar, envíelas por correo electrónico a Documentation-Feedback@netiq.com. Agradecemos sus comentarios y estamos deseando oír sus sugerencias.

Para obtener información de contacto detallada, consulte el sitio web de Información de contacto del servicio técnico.

Para obtener información general sobre productos y la empresa, consulte el sitio web corporativo de NetIQ.

Para mantener conversaciones interactivas con sus colegas y con expertos de NetIQ, hágase miembro activo de nuestra comunidad. La comunidad en línea de NetIQ proporciona información sobre productos, enlaces útiles a recursos interesantes, blogs y canales de redes sociales.

7 Información legal

NetIQ Sentinel está protegido por la patente estadounidense n.º 05829001.

ESTE DOCUMENTO Y EL SOFTWARE DESCRITO EN EL MISMO SE FACILITAN DE ACUERDO CON Y SUJETOS A LOS TÉRMINOS DE UN ACUERDO DE LICENCIA O DE UN ACUERDO DE NO DIVULGACIÓN. EXCEPTO EN LA FORMA ESTABLECIDA EXPRESAMENTE EN EL MENCIONADO ACUERDO DE LICENCIA O ACUERDO DE NO DIVULGACIÓN, NETIQ CORPORATION PROPORCIONA ESTE DOCUMENTO Y EL SOFTWARE DESCRITO EN EL MISMO "TAL COMO ESTÁN" SIN NINGÚN TIPO DE GARANTÍA, YA SEA EXPRESA O IMPLÍCITA,